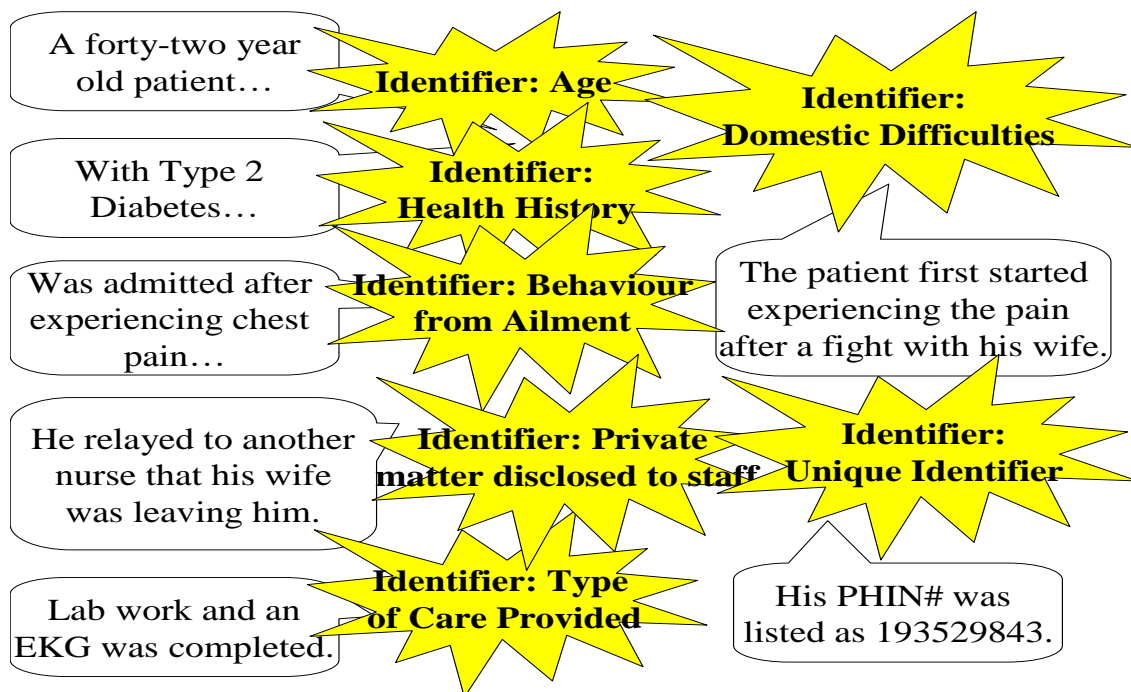


WHAT IS PERSONAL HEALTH INFORMATION?

All information recorded or exchanged verbally about an identifiable individual that relates to:

- The individual's name, health or health care history, including genetic information, about the individual or the individual's family;
- What is learned or observed, including conduct or behaviour, which may be a result of illness or the effect of treatment;
- The provision of health care to the individual. Individuals include co-workers or families of co-workers when they are patients/clients/residents of Southern Health-Santé Sud;
- Payment for health care provided to the individual and includes:
 - The personal health identification number (PHIN) and any other identifying number, symbol or particular assigned to an individual, and
 - Any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care;
- The patient/client/resident's personal information, including financial position, home conditions, domestic difficulties or any other private matters relating to the patient/client/ resident which have been disclosed to staff or persons associated with Southern Health-Santé Sud.

Examples of Personal health information Identifiers:



REMEMBER:

Our patients/clients/residents depend on us to maintain their privacy and keep their personal health information confidential.

Southern Health-Santé Sud, as a Trustee, is bound by Manitoba's *Personal Health Information Act* (PHIA). It is the law. This Act obliges us to protect our patients', clients' and residents' confidentiality and privacy.

While you are performing your duties with Southern Health-Santé Sud, we require that you adhere to the following:

- Keep all patient, client and resident Personal health information confidential and private. Do not discuss any patient, client or resident information with anyone who does not need to know this information to do his or her Southern Health-Santé Sud duties.
- Do not share any patient, client or resident personal health or any other information provided to you;
 - in the presence of someone who does not need to know this information
 - in public places, (i.e., cafeteria, elevators, off premises).



- You are required to ensure that all personal health information is properly secured and maintained to protect its confidentiality and is safe from accidental loss or destruction.
- Authorized personnel who need to transport personal health information outside Southern Health-Santé Sud's premises are required to store laptops, charts, or files in the trunk of their vehicle during transportation or in an out-of-sight location in a locked vehicle if there is no trunk. Personnel must never leave personal health information in the trunk of a vehicle in an area of high risk of theft.
- All confidential material must be disposed of by an approved method (shredding).
- Anyone faxing personal health information needs to take precautions by using the **Record of Access Disclosure Release of Personal Health Information Form** (ORG.1411.PL.502.FORM.03 or ORG.1411.PL.502.FORM.04) – see enclosed samples.
- If you are not sure what is the appropriate thing to do in a specific situation, discuss it with your supervisor, manager, or Privacy Officer/Advisor at your location or the Regional Officer-Privacy and Access at (204) 822-2655 lbassett@southernhealth.ca.
- Report all suspected breaches of confidentiality to your supervisor, manager, or Privacy Officer/Advisor at your location or the Regional Officer-Privacy and Access and complete an occurrence report.



A breach of confidentiality is when you:

- Access or request personal health information NOT NEEDED by you to do your job.
- Provide information NOT NEEDED by the other person to do their job.
- Provide information to an individual who has no right to have the information under PHIA.
- Disclose information to a third party where consent is required and consent has not been obtained from the individual or a person permitted to exercise the rights of the individual.

What is snooping?

Snooping is when an employee, officer or agent of a trustee, information manager or health research organization, disregards the requirement of PHIA and wilfully uses (or attempts to use) personal health information for purposes unrelated to their job duties and contrary to the Act. This includes gaining access or attempting to gain access to another person's personal health information without authorization to do so.

If a breach of confidentiality is confirmed, discipline may include:

- Oral or written warning
- Suspension
- Termination of employment

If convicted of an offence under PHIA, the courts may fine you up to \$50,000.00.

A confirmed breach of confidentiality may be reported to the individual's professional regulatory body.

PHIA POLICIES AT A GLANCE

PHIA DEFINITIONS: To identify which words are defined in PHIA Definitions, (ORG.1411.PL.502.SD.01) these words are capitalized within the policies i.e. Access, Use, Disclosure, etc.



Access to Personal Health Information ORG.1411.PL.101



- **Access means the right of an individual, to examine (view) and receive a copy of the individual's personal health information maintained by the trustee.**
- The provisions of *The Mental Health Act* (Manitoba) take precedence over any conflicting provisions in *The Personal Health Information Act*.
- Individuals have the right to examine, receive copies of, and make corrections to their personal health information.
- Requests for access to information should be in writing to the Privacy Officer/Advisor or designate using the Request to Access Personal Health Information form or in a covering letter which includes the same information.
- Responding to requests for personal health information regarding **care currently being provided:**
 - Where a request to examine personal health information is about a hospital inpatient, a member of the health care team or designate shall make the personal health information available for **examination only** within **24 hours** after receiving the request. Requested copies and explanations must be provided as soon as reasonably possible thereafter.
 - Where a request is from an individual who is not a hospital inpatient (i.e. resident in a personal care home), a member of the health care team or designate shall make the personal health information available for **examination** and if requested, **a copy** of the information must be provided to the requestor within **72 hours** after receiving the request. An explanation must be provided as soon as reasonably possible thereafter.
 - Access must be documented on the health record or on the Request to Access Personal Health Information form.
 - Requests for personal health information may be refused for reasons specified in Section 11 of *The Personal Health Information Act* only.
- A response to all other requests for information must be provided within 30 days and will be coordinated by the Privacy Officer/Advisor or designate.
- The request and response for personal health information shall be included in the individual's health record.

Collection of Personal Health Information ORG.1411.PL.501



- Collect only as much Personal health information as needed to do your job.
- Collect information from the individual the information is about (the policy lists exceptions).
- Collect information in a manner and location that protects the confidentiality, security and integrity of that information.
- A trustee shall inform the individual of the purpose for collecting information and with whom the information will be shared. This may be done by posting notices within the health care facility and/or providing individuals with a brochure or verbally.

Confidentiality of Personal Health Information ORG.1411.PL.201



- To ensure that personal health information is protected so that individuals are not afraid to seek health care or to disclose sensitive information to health professionals.
- To ensure that personal health information is protected during its collection, use, disclosure, storage, and destruction within Southern Health-Santé Sud.
- All employees and persons associated with Southern Health-Santé Sud shall sign a Personal Health Information Declaration of Confidentiality, read the Confidentiality of Personal Health Information policy and complete this self learning package.
- All employees are responsible for protecting the security of all personal health information (oral or recorded in any form) that is obtained, handled, learned, heard or viewed in the course of his/her work or association with Southern Health-Santé Sud.
- Use or disclosure of personal health information is acceptable only in the discharge of one's responsibilities and duties (including reporting duties imposed by legislation) and **based on the need to know**.
- Discussion regarding personal health information shall **not** take place in the presence of persons not entitled to such information or in public places (elevators, lobbies, cafeterias, off premises, etc.).
- Unauthorized use or disclosure of confidential information may result in disciplinary action up to and including termination.

Correction of Personal Health Information ORG.1411.PL.104



- Requests for correction of personal health information must be made in writing to the Privacy Officer/Advisor or designate using the Request to Correct Personal Health Information form or in a covering letter which includes the same information.

Disclosure of Personal Health Information to Police ORG.1411.PL.505



- In most circumstances, police are required to obtain consent for disclosure of personal health information from the individual the personal health information is about or from a person permitted to exercise the rights of that individual. If the police do not have such consent, the police must confirm that charges have been made by completing the Disclosure of Personal Health Information to Police without Consent form or a subpoena, warrant or court order is required before personal health information can be disclosed to police.

- Information may be disclosed to police **without consent** when the police establish that one of the exceptions applies as listed in the policy and when they complete the Disclosure of Personal Health Information to Police Without Consent form.
- To assist police in locating reported missing persons, only the individual's demographic information may be disclosed without consent. This consists of the individual's name, address, email address, and phone number.
- Additional information shall be disclosed as directed by an Emergency Demand for Records form or a Records Access Order produced by the police.
- During normal business hours, requests for disclosure of Personal health information shall be forwarded to a Privacy Officer/Advisor or designate for processing. Requests will be reviewed to determine the urgency of the request and will be processed accordingly.
- After normal business hours, requests (with or without written consent) must be reviewed by the manager in charge to determine the urgency of the request. If the circumstances are urgent, copies of only the portions of the record that are required on an urgent basis should be provided. If the circumstances are not considered to be urgent, the police should be advised to contact the Privacy Officer/Advisor or designate in the Health Information Services Department on the next business day.
- Southern Health-Santé Sud is not obligated to report situations concerning individuals (i.e. discharge of individual, etc.) routinely to the police without individual consent as outlined in the policy.
- Any reporting of persons treated for a gunshot or stab wound shall be in accordance with *The Gunshot and Stab Wounds Mandatory Reporting Act*.

Disposal of Confidential Material, Including Personal and Personal Health Information
ORG.1410.PL.203



- Confidential material must be disposed of by supervised incineration, shredding or other approved methods.

Reporting of Security Breaches Related to Personal Health Information and the Corrective Procedures to be Followed
ORG.1411.PL.203



- If you suspect a breach of confidentiality or security has occurred, immediately notify your supervisor, manager, or Privacy Officer/Advisor at your location or the Regional Officer-Privacy and Access at (204) 822-2655 lbassett@southernhealth.ca.
- The supervisor and/or Human Resources, in consultation with the Regional Officer-Privacy and Access, will determine if the suspected breach should be investigated.
- If a breach has occurred, disciplinary action shall be taken and may include termination.

Retention and Destruction of Personal Health Information
ORG.1410.PL.201



- Personal health information will be retained as per retention periods outlined in the policy.

Security and Storage of Personal Health Information
ORG.1411.PL.404



- Security safeguards shall be in place to protect personal health information, i.e., locked cabinets, restricted access, security clearances, and passwords.
- Users must log off their computers when they leave the workstation.
- Computer users must not share their user IDs and passwords.
- Personal health information shall not be transmitted via e-mail outside the Southern Health-Santé Sud network to a domain that does not partner with the organization to force encryption.

- Files containing personal health information will be kept in a designated secure storage area and not left unattended on desktops.
- Health care providers removing personal health information from the premises on authorized business shall ensure the secure storage of the information at all times.
- All personal health information that is mailed through regular postal service, courier or interdepartmental mail must be marked 'CONFIDENTIAL' and clearly labeled with the name and address of the intended recipient.
- Persons leaving voice messages containing personal health information should be discreet. Personal health information should never be left on a client's voice mail unless the individual whom the information is about has authorized it.

Transmission of Personal Health Information Via Facsimile ORG.1411.PL.407



- Use the Record of Access Disclosure Release of Personal Health Information form ORG.1411.PL.502.FORM.03 or the ORG.1411.PL.502.FORM.04 (Community) whenever faxing Personal health information. Samples are enclosed.
- The sender is responsible for the security of all Personal health information being sent by fax. Ensure the fax number is correct and the fax machine is located in a secure place.
- See Transmission of Personal health information via Fax Checklist ORG.1411.PL.407.SD.01 (sample enclosed).

Use and Disclosure of Personal Health Information ORG.1411.PL.502



- **Use is revealing personal health information to someone within Southern Health-Santé Sud.**
- **Disclosure is revealing personal health information to someone outside of Southern Health-Santé Sud.**
- Before using or disclosing personal health information, reasonable steps must be taken to ensure the information is accurate, up to date, complete and not misleading.
- Use of personal health information is limited to "the need to know" for your job.
- Requests for disclosure of personal health information are coordinated with the Privacy Officer/Advisor or designate.
- A record of all personal health information disclosed shall be kept on the health record.
- The individual's consent is required to disclose personal health information except under circumstances listed in the policy.
- Personal health information may be disclosed without consent if authorized or required to do so by an enactment of Manitoba or Canada, for example, *The Child and Family Services Act*, *The Fatality Inquiries Act*.
- PHIA allows disclosure to any person an individual's name, condition and location (as long as the location does not reveal specific information about the individual) as long as it is not contrary to the express request of the individual or his or her representative.
- PHIA allows for demographic information or the PHIN to be used to confirm eligibility for health care or payment for health care or verifying the accuracy of the demographic information or PHIN.

Take Our Kids to Work Day ORG.1511.PL.006



- A parent who wishes to bring a student to work shall request permission in advance from their designated management representative.
- Once approved the student and parent must sign the Take Our Kids to Work Agreement and Undertaking and complete this PHIA Self Learning Package.



- An individual who wishes to job shadow within Southern Health-Santé Sud shall submit a written request for permission in advance to the staff/physician they wish to shadow and the supervisor/manager of that program where the observer will be in attendance.
- The observer must read the Confidentiality of Personal Health Information policy.
- The observer must read and sign the Southern Health-Santé Sud Personal Health Information & Agreement for Job Shadowing form and if deemed necessary, read and sign the Southern Health-Santé Sud Declaration of Confidentiality form.

**Personal health information Act (PHIA)
Self Learning Quiz**

Please circle the correct answer:

- T F 1. The *Personal health information Act* is also referred to as PHIA.
- T F 2. The Personal health information Act provides protection against abuse for employees in Regional Health Authorities and other government agencies.
- T F 3. The Personal health information Act (PHIA) is a provincial law that protects the privacy of an individual's identifiable personal health information
- T F 4. Southern Health-Santé Sud is a Trustee of personal health information.
- T F 5. It is considered a breach of confidentiality if a client's name is released to the media without prior consent.
- T F 6. An employee must report breaches of confidentiality "to the privacy officer" appointed to the site/area or the Regional Officer-Privacy and Access.
- T F 7. You may ONLY use/disclose personal health information when you:
 - a) have consent from the individual the personal health information is about;
 - b) are a person permitted to exercise the rights of an individual; or
 - c) you are entitled by PHIA or other legislation.

<i>Acknowledgement of Completion</i>		
I have reviewed the policy, attachments and quiz related to The Personal health information Act.		
Employee/Student Name (Please print)	Employee #	Site/Program
Employee/Student Signature	Facilitator Signature	
Date: _____	Date: _____	

Facility/Program Staff: Please forward completed form to Education Facilitator/Supervisor.

**Corporate/Regional Office's and Home Care please forward completed QUIZ to:
Southern Health-Santé Sud
ATTN: Staff Development
3-30 Stephen Street
Morden MB R6M 2G3**

Answers: 1) T 2) F 3) T 4) T 5) T 6) T 7) T



RECORD OF ACCESS DISCLOSURE RELEASE OF PERSONAL HEALTH INFORMATION FORM

To: _____
 Fax #: _____
 Phone# _____

From: _____
 Date: _____
 Pages: _____ (including this cover page)

Client Name: _____

Health Record # _____
 Date of Birth: _____ (dd/mmm/yy)

Reason for Disclosure: Transfer Referral Other _____

Information Disclosed by: Fax Mail Sent with Client Other _____

INFORMATION DISCLOSED (Check all that apply and include applicable dates/timeframes of report(s) disclosed):

Date of Report

- Consultation Report _____
- Discharge Summary _____
- ED/OPD Record _____
- History & Physical _____
- Operative Report _____
- Referral Letter _____

Date of Report

- Other Prenatal Record _____
- Pathology Report _____
- Other _____

DIAGNOSTIC IMAGING

- CT Scan _____
- MRI _____
- Ultrasound _____
- X-ray _____
- Mammogram _____
- Other _____

DIAGNOSTICS

- Chemistry _____
- EKG _____
- Hematology _____
- Microbiology _____
- Urinalysis _____
- FOBT _____
- Urine C&S _____
- Other _____

The client documents accompanying this transmission contain confidential information intended for a specific individual and purpose. The information is private and is legally protected by law. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this transmission is strictly prohibited. If you have received this communication in error, please notify us immediately and return the original transmission to us. Thank you.



RECORD OF ACCESS DISCLOSURE RELEASE OF PERSONAL HEALTH INFORMATION (COMMUNITY) FORM

To: _____

From: _____

Fax #: _____

Date: _____

Phone# _____

Pages: _____ (including this cover page)

Client Name: _____

Health Record # _____

Date of Birth: _____ (dd/mmm/yy)

Reason for Disclosure: Transfer Referral Other _____

Information Disclosed by: Fax Mail Sent with Client Other _____

INFORMATION DISCLOSED (Check all that apply and include applicable dates/timeframes of report(s) disclosed):

Date of Report

Date of Report

Assessment _____

Consult Record _____

Discharge Summary _____

Immunizations _____

Letter _____

Memo _____

Progress Note _____

Referrals _____

Other _____

The client documents accompanying this transmission contain confidential information intended for a specific individual and purpose. The information is private and is legally protected by law. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this transmission is strictly prohibited. If you have received this communication in error, please notify us immediately and return the original transmission to us. Thank you.

BEFORE Faxing You Must:

1. Make sure the documents you are faxing include a fax cover sheet that:
 - Clearly identifies who is sending the fax; (Sender name)
 - Clearly identifies who the fax is going to; (Recipient)
 - Records the total number of pages being faxed (including the coversheet); and
 - States the site approved confidentiality statement.
2. Double check that you have the correct fax number for the person you are sending the fax to.
3. Once you have keyed the fax number; confirm it is the correct number before pressing the “send” button.

AFTER Faxing You Must:

1. Remove the documents from the fax machine, no documents containing personal health information should ever be left unattended on a fax machine.
2. Check the fax confirmation sheet or display to make sure that all the pages were successfully sent and that they went to the correct recipient.
3. When a fax contains extremely sensitive information, contact the receiver prior to faxing and to confirm receipt of the fax.

RECEIVING Faxed Documents:

1. Remove the documents from the fax machine as soon as possible. Documents containing personal health information should not be left unattended on a fax machine that is not located in a secure area that is only accessible by Southern Health-Santé Sud staff.
2. Check to make sure that all pages sent to your site were received.

When personal health information is mistakenly faxed to the wrong site or person (Recipient) you MUST notify your supervisor, manager or site Privacy Officer/Advisor immediately to report the breach.

Personal health information Declaration of Confidentiality

I, the undersigned, have read and understand the Southern Health-Santé Sud policy on confidentiality of personal health information as described in the Confidentiality Policy which is in accordance with *The Personal health information Act* (Manitoba).

I also acknowledge that I am aware of and understand the Corporate Policies of Southern Health-Santé Sud regarding the security of personal health information including the policies relating to the use, collection, disclosure, storage and destruction of personal health information.

In consideration of my employment or association with Southern Health-Santé Sud, and as an integral part of the terms and conditions of my employment or association, I hereby agree, declare and undertake that I will not at any time, during my employment or association with Southern Health-Santé Sud, or after my employment or association ends, access or use personal health information, or reveal or disclose to any persons within or outside Southern Health-Santé Sud, any personal health information except as may be required in the course of my duties and responsibilities and in accordance with applicable Legislation, and Corporate and departmental policies governing proper release of information.

I understand that my obligations outlined above will continue after my employment/ contract/ association/ appointment with Southern Health-Santé Sud ends.

I further understand that my obligations concerning the protection of the confidentiality of personal health information relate to all personal health information whether I acquired the information through my employment/contract/association/appointment with Southern Health-Santé Sud or within any of the healthcare facilities within Southern Health-Santé Sud.

I also understand that unauthorized use or disclosure of such information may result in a disciplinary action up to and including termination of employment/contract/association/appointment, the imposition of fines pursuant to *The Personal health information Act*, and where applicable, a report to my professional regulatory body.

I have read and understand the contents of the Southern Health-Santé Sud Personal health information Confidentiality Policy and the consequences of a breach.

This declaration was made by: _____	_____																				
	Position held and Location (Facility/Office)																				
Signature: _____	Date: <table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px; height: 20px;"> </td> <td style="width: 20px; height: 20px;"> </td> <td style="width: 20px; height: 20px;"> </td> <td style="width: 20px; height: 20px;"> </td> <td style="width: 20px; height: 20px;"> </td> <td style="width: 20px; height: 20px;"> </td> <td style="width: 20px; height: 20px;"> </td> <td style="width: 20px; height: 20px;"> </td> <td style="width: 20px; height: 20px;"> </td> <td style="width: 20px; height: 20px;"> </td> </tr> <tr> <td>D</td><td>D</td><td>M</td><td>M</td><td>M</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td><td></td> </tr> </table>											D	D	M	M	M	Y	Y	Y	Y	
D	D	M	M	M	Y	Y	Y	Y													

I have provided the applicable PHIA education as it relates to the Confidentiality Policy and explained the consequences of a breach with the above named.

_____	_____
Witness Signature	Print Name and Title of Witness